Exhibit G

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

--- X:

SIMO HOLDINGS INC.,

Plaintiff, : No. 1:18-cv-05427 (JSR)

-against-

HONG KONG UCLOUDLINK NETWORK
TECHNOLOGY LIMITED and
UCLOUDLINK (AMERICA), LTD.,

Defendants. X

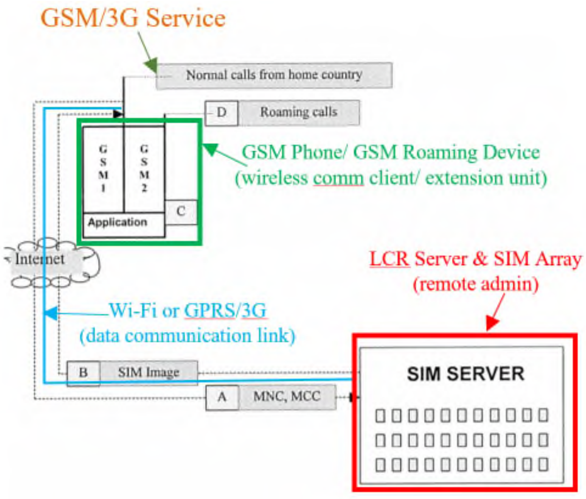
INVALIDITY REPORT OF MARTIN J. FEUERSTEIN

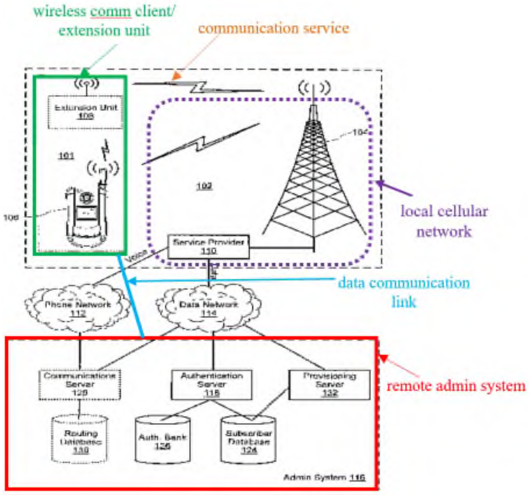
information, the communications device could get registered with the local network and is able to "place telephone calls" and obtain "[a]ll mobile services." *Id.* at ¶ 29. Since the shared authentication information is from a SIM card that is remotely located but issued by "[a] mobile cellular telephone service provider…in a local region" (*id.* at ¶ 38), the communications terminal is therefore operated "as if it were a local communication client" as described by the '689 Patent ('689 patent at 4:66-5:1).

C. Overview of *Walton*

67. International Application Publication No. WO 2006/094564 A1 to Walton ("*Walton*") was published on September 14, 2006, which is more than one year before the earliest priority date of the '689 patent. *Walton* qualifies as prior art to the '689 patent under 35 U.S.C. § 102(b).

68. As illustrated below, *Walton* discloses a call routing method for roaming devices implemented by a remote virtual SIM card system, which is substantially the same as the mobile telephone roaming method in the '689 patent implemented by the foreign wireless communication system:





Walton at FIG. 1 ’689 Patent at FIG. 1

69. *Walton* recognized the same problem of high roaming cost that the ’689 patent recognized, (*Walton* at 1:18-19.) and solved the problem in the same way. In particular, this GSM roaming device “does not physically contain a GSM SIM card.” *Id.* at 4:13-14. Instead it relies on a remote “SIM Card Array,” using a SIM card stored in the SIM Card Array which is “a device for central storage of and remote access to any number of SIM cards.” *Id.* at 3:6-7, 4:17-18. “All communication between the GSM engine and the SIM card is relayed over the Internet (back and forth) between one of the SIM Cards physically located in the remote SIM Card Array.” *Id.* at 4:15-18.

70. The remote physical SIM card used in *Walton* to enable wireless communication is subscribed to a local carrier of a current location (*id.* at 8:28-9:6) while the GSM phone and GSM Roaming device are not. *Id.* at 12:31-13:11.

76. More specifically, the authentication request (authentication message RAND) and authentication information (response message SRES) in *Kasper* is consistent with specification of the ’689 Patent. ’689 Patent at 11:53-61. In *Kasper*, the mobile device initiates an authentication process with a network operator by “relay[ing] $IMSI_i$” to the network operator. *Kasper* at page 59. The network then “replies” to the mobile device with an authentication request in the form of “authentication challenge $RAND_i$.” *Id.* The authentication request is then “passed to” a relevant function of the Mobile Trusted Platform in order to derive an authentication information in the form of “challenge response message SRES*.” *Id.* The server “sends” the authentication information to the mobile terminal, which will “relay” it to the network operator. *Id.* The mobile device is subsequently “authenticated” by the network operator and obtains “access in mobile cellular networks” as if it is a local wireless device. *Id.* at page 59 and 57.

IX. INVALIDITY OVER THE PRIOR ART

A. *Andreini* Anticipates, or Alternatively *Andreini* in View of *Walton* Renders Obvious, Claims 8 and 11-13

77. As explained below, it is in my opinion that *Andreini* discloses each and every element of claims 8 and 11-13, either expressly or inherently, and thus anticipates these claims. Or alternatively, to the extent of the preamble of independent claim 8 is limiting, *Andreini* in view of *Walton* discloses, suggests, or teaches all elements of claims 8 and 11-13, and thus renders these claims obvious.

1. Claim 8

a. “A wireless communication client or extension unit comprising a plurality of memory, processors, programs, communication circuitry, authentication data stored on a subscribed identify module (SIM) card

and/or in memory and non-local calls database, at least one of the plurality of programs stored in the memory comprises instructions executable by at least one of the plurality of processors for"

78. *Andreini* discloses the preamble of claim 8. Or alternative, *Andreini* in view of *Walton* discloses the preamble of claim 8, to the extent the preamble is limiting. As shown in FIGS. 2 and 3 (reproduced below), *Andreini* discloses a peripheral device 13 (i.e., the "wireless communication client or extension unit" of claim 8) comprises: a memory unit 20 acting as a virtual SIM card (*Andreini* at ¶ 38) and a RAM unit 22 (*id*. at ¶ 41) (i.e., the "memory" of claim 8); CPU 16 (*id*. at ¶ 41) (i.e., the "processors" of claim 8); radio unit 17 (GSM1) equipped with a resident SIM card 19 and radio unit 18 (GSM2) connected to virtual SIM card 20 (*id*. at ¶¶ 37-38) (i.e., "communication circuitry" of claim 8); and "authentication parameters in the memory unit, 20" (*id*. at ¶ 41) (i.e., "authentication data stored on a subscribed identify module (SIM) card and/or in memory" of claim 8).

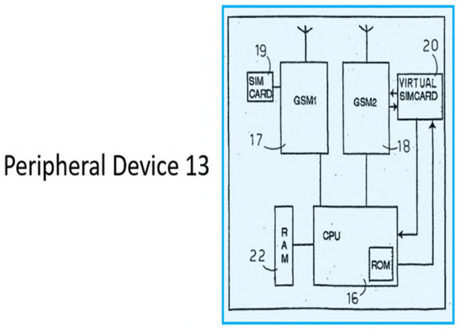


FIG.2

Foreign Wireless Communication Client or Extension Unit

Foreign Wireless Communication Client or Extension Unit

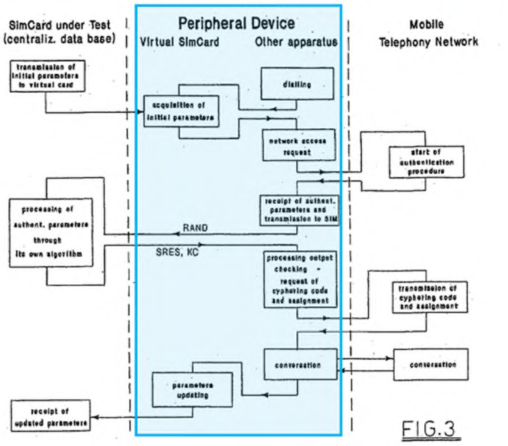

SimCard under Test (centraliz. data base)
Peripheral Device
Virtual SimCard
Other apparatus
Mobile Telephony Network
transmission of initial parameters to virtual card
dialling
acquisition of initial parameters
network access request
start of authentication procedure
processing of authent. parameters through its own algorithm
receipt of authent. parameters and transmission to SIM
RAND
SRES, KC
processing output checking - request of cyphering code and assignment
transmission of cyphering code and assignment
conversation
conversation
parameters updating
receipt of updated parameters

FIG.3

79. *Andreini* further teaches programs which are stored in the memory comprising instructions executable by processors. For example, "CPU, 16, stores the above mentioned authentication parameters in the memory unit, 20, which module, 18, interfaces with during the verification. The verification start up time and the telephone number to dial for performing the verification are stored in the RAM unit, 22, of the CPU, 16." *Id.* at ¶41.

80. To the extent the preamble is limiting, a PHOSITA reviewing *Andreini* would have known that the peripheral device 13 in *Andreini* also needs a non-local calls database. In particular, a PHOSITA reviewing *Andreini* would have been motivated to look at other references, such as *Walton*, to find the details regarding how to make a non-local call.

81. The '689 patent describes a non-local calls database. For example, the '689 patent explained that "[t]he non-local calls database 525 lists **various locations**, **corresponding area codes**, and corresponding **local dial-in telephone numbers** for use when the subscriber wants to make a non-local call when present at a particular location." '689 patent at 15:55-60. The '689 patent further explains that "[w]hen a user desires to make a non-local call when within a particular location (e.g., a visiting caller in London wants to call his home office in San Francisco), the client 106 or extension unit 108 is able to determine that the called number is not within the local area, and then **dial a local communication server 128 (FIG. 1) at a local number from the list**." *Id.* at 60-65. Therefore, the non-local calls database is a database comprising of information like various locations, corresponding area codes, and corresponding local dial-in telephone numbers, by which a non-local call is detected and the client or extension unit dials a local communication server at a local number from the database.

82. Likewise, *Walton* discloses a method "comprises means designed to detect when a call is being made by the GSM phone, to delay the GSM phone from making the call

generally to “mobile telecommunication systems, and in particular to a system and method for operating a foreign mobile telecommunications device in a local communication network as if it were a local mobile telecommunications device.” ’689 patent at 1:15-20.

85. *Andreini* discloses that “[m]ain aim of this invention is to propose an apparatus, and corresponding method, for verifying the procedure to access mobile telephony networks through SIM cards **overcoming the limitation of low availability of cards itself and the need of placing them at the various locations of the managed network area.**” *Andreini* at ¶7.

Similarly, the general purpose of *Walton* is to “provide a method for rerouting mobile phone communications, which involves least cost routing of the communications.” *Walton* at 3:15-20.

86. Second, *Andreini* already discloses that the invention supports “the required type of phone communication among the available kinds of transmissions and services.” It details how to make a non-local call but does not discuss how to achieve least cost. *Walton* simply aims to make outbound phone calls with least cost by rerouting mobile phone communications and particularly discloses the limitation of non-local calls database (e.g., Calling Line Identification (CLI); Dialed Number Identification (DNI); and a diverting number). *Walton* at 7:15-20. Therefore, it would be obvious for a PHOSITA to modify the peripheral device 13 by adding a non-local calls database taught by *Walton*. Such a modification could quickly and easily be achieved with predictable results, as it would merely require minor changes to *Andreini.*

87. Therefore, in my opinion, *Andreini* in view of *Walton* fully teaches the preamble of claim 8 to the extent that the preamble is limiting. Otherwise, *Andreini* discloses the preamble.

b. “enabling an initial setting of the wireless communication client or the extension unit and a remote administration system”

126. Second, *Andreini* already discloses a specific verification request for some specific parameters such as IMSI, TMSI, or **similars** for the purpose of authentication. See *Andreini* at ¶40, 8. Obviously, "similars" means that the aforesaid authentication parameters are not limited to the listed items. Accordingly, a PHOSITA would be motivated to look into other references like *Shi* and/or *Walton* to add some other common authentication information. It would be obvious for a PHOSITA to modify *Andreini* by adding password, locations, or wireless communication client identifier as taught by *Shi* and/or *Walton* as authentication information. Such a modification could quickly and easily be achieved with predictable results, as it would merely require minor changes to *Andreini.* Third, the number of authentication parameters stored in the SIM card is finite. It would be obvious for a PHOSITA to choose password, locations or wireless communication client identifier as authentication parameters from a finite number of identified, predictable items, with a reasonable expectation of success.

127. Thus, *Andreini* in view of *Shi* or (*Shi* and *Walton*) discloses all elements of claim 14, and thus renders claim 14 obvious.

C. *Patarkazishvili* Anticipates, or Alternatively *Patarkazishvili* in View of *Walton* Renders Obvious, Claims 8 and 11-13

128. As explained below, it is in my opinion that *Patarkazishvili* discloses each and every element of claims 8 and 11-13, either expressly or inherently, and thus anticipates these claims. Or alternatively, to the extent of the preamble of independent claim 8 is limiting, *Patarkazishvili* in view of *Walton* discloses, suggests, or teaches all elements of claims 8 and 11-13, and thus renders these claims obvious.

1. Claim 8

a. "A wireless communication client or extension unit comprising a plurality of memory, processors, programs, communication circuitry, authentication data stored on a subscribed identify module (SIM) card and/or in memory and non-local calls database, at least one of the plurality of programs stored in the memory comprises instructions executable by at least one of the plurality of processors for"

129. *Patarkazishvili* discloses the preamble of claim 8. Or alternatively, *Patarkazishvili* in view of *Walton* discloses the preamble of claim 8, to the extent the preamble is limiting. For example, *Patarkazishvili* discloses a "computerized communications terminal which communicates over the radio frequency (RF) interface of the cellular telephone network." (the "wireless communication client or extension unit" of claim 8). *Patarkazishvili* at ¶ 27. Further, *Patarkazishvili* defines that a computer or computer system may include a single physical device (such as a mobile phone or Personal Digital Assistant) where internal modules such as a memory and processor (the claimed "memory" and "processor") work together performing operations on electronic data. *See id.* ¶ 34. Because it's a computerized communications terminal, communication circuitry must have been included. Besides, a computer system can comprise computer-readable media which is used to carry or store desired program code means in the form of computer-executable instructions. *See id* ¶ 32 ("Embodiments within the scope of the present invention also include computer-readable media for carrying or having computer-executable instructions, computer-readable instructions, or data structures stored thereon.").

130. Moreover, *Patarkazishvili* teaches authentication data stored on a subscribed identify module (SIM) card and/or in memory (e.g., the communications terminal includes a subscriber identity module (SIM) emulator emulating the SIM card inserted in a client computer based on the SIM identification data at the communications terminal). *See id.* ¶ 18 ("The

135. A PHOSITA would be motivated to combine *Patarkazishvili* with *Walton* at the time of the invention for several reasons. First, *Patarkazishvili* and *Walton* are in the same field of endeavor as the '689 patent directed to a mobile roaming device. For example, the '689 patent relates generally to "mobile telecommunication systems, and in particular to a system and method for operating a foreign mobile telecommunications device in a local communication network as if it were a local mobile telecommunications device." Ex. 1001 at 1:15-20.

136. *Patarkazishvili* "intended to provide a system and method for making and receiving telephone calls while traveling or roaming away from home." *Patarkazishvili* at ¶29. Similarly, the general purpose of *Walton* is to "provide a method for rerouting mobile phone communications, which involves least cost routing of the communications." *Walton* at 3:15-20.

137. Second, *Patarkazishvili* simply aims to enable "roaming user can receive and place telephone calls through an Internet connection but only locally through the home region the cellular telephone network." *Patarkazishvili* at ¶29. But it lacks details how to make a non-local call. *Walton* is designed for making outbound phone calls with least cost by rerouting mobile phone communications and particularly discloses the limitation of non-local calls database (e.g., Calling Line Identification (CLI), Dialed Number Identification (DNI), and diverting number). *See Walton* at 7:15-20. Therefore, it would be simple for a PHOSITA to add a non-local calls database to *Patarkazishvili* as taught by *Walton*. Such a modification could quickly and easily be achieved with predictable results, as it would merely require minor changes to *Patarkazishvili.*

138. Therefore, in my opinion, *Patarkazishvili* in view of *Walton* fully teaches the preamble of claim 8.

b. "enabling an initial setting of the wireless communication client or the extension unit and a remote administration system"

139. *Patarkazishvili* discloses this element of claim 8. For example, *Patarkazishvili*

of *Walton* is to "provide a method for rerouting mobile phone communications, which involves least cost routing of the communications." *Walton* at 3:15-20.

174. Second, *Patarkazishvili* discloses that "[t]he authentication information is required for authenticating the SIM module by the local cellular mobile telephone operator." *Patarkazishvili* at ¶17. A PHOSITA would know that the aforesaid authentication information is not limited to a unique subscriber identifier. Accordingly, a PHOSITA would be motivated to look into other references like *Shi* and *Walton* to add some other common authentication information. It would be obvious for a PHOSITA to modify *Patarkazishvili* by adding the claimed "wireless communication client identifier, a password, and a current location of the foreign wireless communication client or the extension unit" as taught by *Shi* and *Walton* as authentication information. Such a modification could quickly and easily be achieved with predictable results, as it would merely require minor changes to *Patarkazishvili.*

175. Third, the number of authentication information is finite. It would be obvious for a PHOSITA to choose others like wireless communication client identifier, a password, and a current location of the foreign wireless communication client or the extension unit as authentication information from a finite number of identified, predictable items, with a reasonable expectation of success.

176. Thus, *Patarkazishvili* in view of *Shi* and *Walton* discloses all elements of claim 14, and thus renders claim 14 obvious.

E. *Kasper* in view of *Walton* Renders Claims 8 and 11-13 Obvious

177. As explained below, it is in my opinion that *Kasper* in view of *Walton* discloses all elements of claims 8 and 11-13, and thus renders these claims obvious.

1. Claim 8

a. "A wireless communication client or extension unit comprising a plurality of memory, processors, programs, communication circuitry, authentication data stored on a subscriber identify module (SIM) card and/or in memory and non-local calls database, at least one of the plurality of programs stored in the memory comprises instructions executable by at least one of the plurality of processors for:"

178. *Kasper* in view of *Walton* teaches the preamble of claim 8, to the extent the preamble is limiting. *Kasper* describes a mobile device/mobile station/GSM client (i.e., the "wireless communication client or extension unit" of claim 8). According to *Kasper*, the mobile device/mobile station/GSM client can be a mobile phone equipped with a SIM emulation adapter (*id.* at page 5, ¶ 5) and a hardware chip called MTM (mobile trusted module, *id.* at page 1, ¶ 1). The client therefore has a memory (e.g., non-volatile memory of MTM, *id.* at page 24, ¶ 2; page 28, ¶ 5), processors (e.g., secure co-processor, *id.* at page 37, ¶ 1), programs (e.g., trusted software layer of MTM, *id.* at page 37, ¶ 3), and communication circuitry (e.g., circuitry at least for establishing internet connection, *id.* at page 5, ¶ 5). In addition, the memory of MTM is capable of storing authentication data such as vSIM credential. *Id*. at page 78, ¶¶ 1-2 ("Protection of the vSIM Credential during execution… the secret individual key Ki would never leave the hardware protected environment of the MTM.").

179. *Kasper* provides that its "model could be implemented in conventional GSM clients without any technological changes at the GSM infrastructure and at the GSM authentication protocol." *Id.* at page 57, ¶ 1. Therefore, a PHOSITA would recognize that the GSM client in *Kasper*, corresponding to the "wireless communication client or extension unit" of claim 8, would at least have a voice call function, just like a conventional GSM phone would do. However, *Kasper* is silent on whether the GSM client has a non-local call database to facilitate its voice call function. But it is well known that at the time of the purported invention of '689

patent (for example, February 2008), calls made by GSM phones to a local area and a non-local area are billed and charged differently.

180. The ’689 patent described non-local calls database. For example, the ’689 patent explained that “[t]he non-local calls database 525 lists **various locations**, **corresponding area codes**, and corresponding **local dial-in telephone numbers** for use when the subscriber wants to make a non-local call when present at a particular location.” Ex. 1001 at 15:55-60. The ’689 patent further explains that “[w]hen a user desires to make a non-local call when within a particular location (e.g., a visiting caller in London wants to call his home office in San Francisco), the client 106 or extension unit 108 is able to determine that the called number is not within the local area, and then **dial a local communication server 128 (FIG. 1) at a local number from the list**.” *Id.* at 60-65. Therefore, the non-local calls database is a database comprising of information like various locations, corresponding area codes, and corresponding local dial-in telephone numbers, by which a non-local call is detected and the client or extension unit dials a local communication server at a local number from the database.

181. Likewise, *Walton* discloses a method “comprises means designed to detect when a call is being made by the GSM phone, to delay the GSM phone from making the call immediately, to send an IP message, containing the **Calling Line Identification (CLI)** corresponding to the calling GSM phone” (i.e. the “local dial-in telephone numbers” of the ’689 patent), and “the **Dialed Number Identification (DNI)** corresponding to the correspondent phone line” (i.e., the “various locations, corresponding area codes” of the ’689 patent) “**to a dedicated server**” **(**i.e., the “local communication server” of the ’689 patent). *Walton* at 7:15-20.

182. Additionally, *Walton* discloses a local dial-in telephone number (e.g., the diverting number):

> (2) delay the GSM phone from making the call immediately,
>
> (3) send an IP message, containing the Calling Line Identification (CLI) corresponding to the calling GSM phone, and the Dialled Number Identification (DNI) corresponding to the Correspondent phone line, to the LCR Management Server,
>
> (4) have the LCR Management Server **send a diverting number** (of the Telecom witch) **to the GSM phone**.
>
> (5) have the GSM phone call **the diverting number** and the Telecom Switch receive the call;
>
> (6) have the Telecom Switch call the DNI sent in step (3) and connect the call.

Id. at 15:29-16:8 (emphases added). Whereas, the diverting number is a "local dial-in telephone number[]" of the '689 patent.

183. Therefore, a PHOSITA would have been motivated to consider to have a non-local database on the GSM client of *Kasper* to use the non-local database to differentiate local and non-local calls so they can be billed and charged differently. One of such reference that a PHOSITA would have considered is *Walton*, which is also directed to a GSM Phone (i.e., wireless communication client) and a GSM Roaming Device (i.e., extension unit). According to Walton, the GSM Phone has memory (e.g., a MNC/MCC memory and a memory for storing a GSM Phone Application Software Program, Walton at 6:23-30), processors (e.g., processors including the one executing the GSM Phone Application Software Program, *id.* at 8:20-21), programs (e.g., programs including the GSM Phone Application Software Program, *id.* at 8:20-21), and communication circuitry (e.g., including at least the WPAN and WLAN chips, *id.* at

4:8-10). The GSM Phone in Walton additionally includes authentication data stored on a subscribed identify module (SIM) card (e.g., a SIM card that stores unique identity code, *id.* at 7:28-29, 2:27-34). *Walton* is designed for making outbound phone calls with least cost by rerouting mobile phone communications and particularly discloses the limitation of non-local calls database (e.g., Calling Line Identification (CLI), Dialed Number Identification (DNI), and diverting number). *See Walton* at 7:15-20.

184. In addition, a PHOSITA would have appreciated the similarity in approach of *Kasper* and *Walton,* which involve the way of requesting and providing authentication information of a SIM card. Same in both references, the SIM card used by a mobile device to authenticate itself in a local network is not inserted into or physically attached to the mobile device. Instead, the SIM cards are placed in a remote location and SIM data are transmitted over a wireless data connection. Both *Kasper* and *Walton* use such approach to eliminate the restriction of traditional physical SIM and provide a more flexible way for local mobile device to obtain authentication data that it needs.

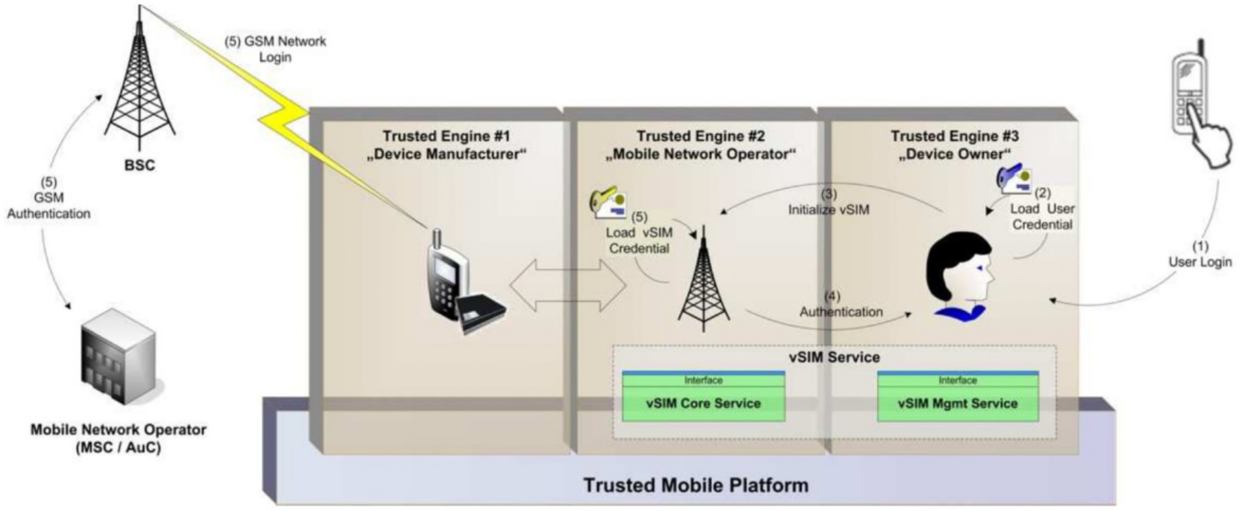
185. Therefore, a PHOSITA would have deemed it obvious to use the GSM phone or GSM roaming device of *Walton* to implement the GSM client of *Kasper.* In *Walton*, when the GSM Phone tries to make an outbound call or receive an incoming call, the system implements different methods of routing for local calls (*Walton* at 7:6-8 ("to fixed line or mobile numbers that are in the same local area of the mobile network corresponding to the virtual SIM")) and non-local calls (*id.* at 7:9-11 ("other outbound calls")). Therefore, the GSM phone has to contain a non-local calls database.

186. For all of these reasons, a PHOSITA would have been motivated to combine *Kasper* and *Walton* and deemed it obvious to implement the GSM client of *Kasper* in the same

way as GSM Phone or GSM Roaming Device of *Walton*, namely, implementing the GSM client of *Kasper* as having a non-local call database.

b. "enabling an initial setting of the wireless communication client or the extension unit and a remote administration system"

187. *Kasper* discloses this element of claim 8. *Kasper* discloses enabling an initial setting by "initialize[ing] the vSIM services and perform[ing] a log-in sequence". *Kasper* at page 58, ¶ 1. The initial setting is conducted between a mobile device and a trusted subsystem TSSu of a Mobile Trusted Platform (MTP). The trusted subsystem TSSu "holds a vSIM$_{MGMT}$ service" that is "responsible for administration and authentication of local users." Id. at page 58, page 42, paras. 1-2. According to *Kasper*, "Once, the vSIMCORE has received the signed message, it verifies its status. Finally, the vSIMCORE unseals CredvSIM and initializes the SIM functionality using the IMSI$_i$ and Ki (Step5)." *Id.* at page 59, ¶ 1. Such process is also illustrated as Step 1 through Step 5 in Figure 3.8 (reproduced below).



c. "establishing a data communication link to transmit information among the wireless communication client or the extension unit, and the remote administration system"

188. *Kasper* discloses this element of claim 8. *Kasper* also establishing a data communication link between the wireless communication client and the remote administration system. According to *Kasper*, "client uses an already established internet connection and connects to the central SIM server in order to relay the authentication messages." *Kasper* at page 5, ¶ 5. More specifically, *Kasper* provides that such connection can be implemented as "existing PAN (e.g. Bluetooth) as well as an established connection to the destination device over the internet." *Id.* at page 80, ¶ 2. To sum up, there is a data communication link (e.g., an internet connection or Bluetooth) connecting the wireless communication device (e.g., GSM client) and remote administration system (e.g., Central SIM server such as mobile trusted platform).

d. "establishing a local authentication information request in response to a local authentication request by a local cellular communication network, wherein the local authentication information request comprises information regarding the local authentication request for local authentication information received by the foreign wireless communication client or the extension unit from the local cellular communication network"

189. *Kasper* discloses this element of claim 8. *Kasper* discloses establishing a local authentication information request in response to a local authentication request by a local cellular communication network. In *Kasper*, the mobile device "requests for authentication at the GSM network" (*Kasper* at page 59, ¶ 4) and receives an authentication challenge RAND_i from the GSM network (i.e., the "information regarding the local authentication request for local authentication information received by the foreign wireless communication client or the extension unit from the local cellular communication network" of claim 8). *Id.* at page 59, ¶ 4. RAND_i is "information of identification and authentication of a subscriber" used by Authentication Center of GSM network. *Id.* page 11, ¶ 2. In response to RAND_i, the mobile

device establishes and relays an authentication message (i.e., the "local authentication information request" of claim 8) including at least the RAND$_i$ to vSIM$_{CORE}$ (i.e., "establishing a local authentication information request" of claim 8). *Id.* at page 59, ¶ 6 ("This RAND$_i$ is passed to the trusted vSIMCORE service."), at page 5, ¶ 5 ("While performing network authentication, the client…connects to the central SIM server in order to relay the authentication messages").

e. "and wherein the data communication link is distinct from the local cellular communication network"

190. *Kasper* discloses this element of claim 8. In *Kasper*, the data communication link between mobile device and the smart card server can be a Bluetooth connection or an established internet connection, which is distinct from local wireless services of the local carrier. *Kasper* at page 5, ¶ 5, and page 80, ¶ 4.

f. "relaying the local authentication information request to the remote administration system via the data communication link and obtaining suitable local authentication information from the remote administration system via the data communication link"

191. *Kasper* discloses this element of claim 8. *Kasper* discloses sending the authentication message including at least the RAND$_i$ to vSIM$_{CORE}$ (i.e., "relaying the local authentication information request to the remote administration system" of claim 8). *Id.* at page 59, ¶ 6 ("This RAND$_i$ is passed to the trusted vSIMCORE service."), at page 5, ¶ 5 ("While performing network authentication, the client uses an already established internet connection and connects to the central SIM server in order to relay the authentication messages"). The message is relayed using the established internet connection (i.e., "the data communication link" of claim 8). *Id.* page 5, ¶ 5.

192. *Kasper* also discloses obtaining an authentication challenge response message SRES* from vSIM$_{CORE}$ (i.e., "obtaining suitable local authentication information from the remote

administration system" of claim 8). *Id.* at page 59, ¶ 6 ("The output of the algorithm is the challenge response message SRES*. The vSIMCORE sends this SRES* message to the MNO.), at page 5, ¶ 5 ("While performing network authentication, the client uses an already established internet connection and connects to the central SIM server in order to relay the authentication messages"). The response message is also obtained using the established internet connection (i.e., "the data communication link" of claim 8). *Id.* page 5, ¶ 5.

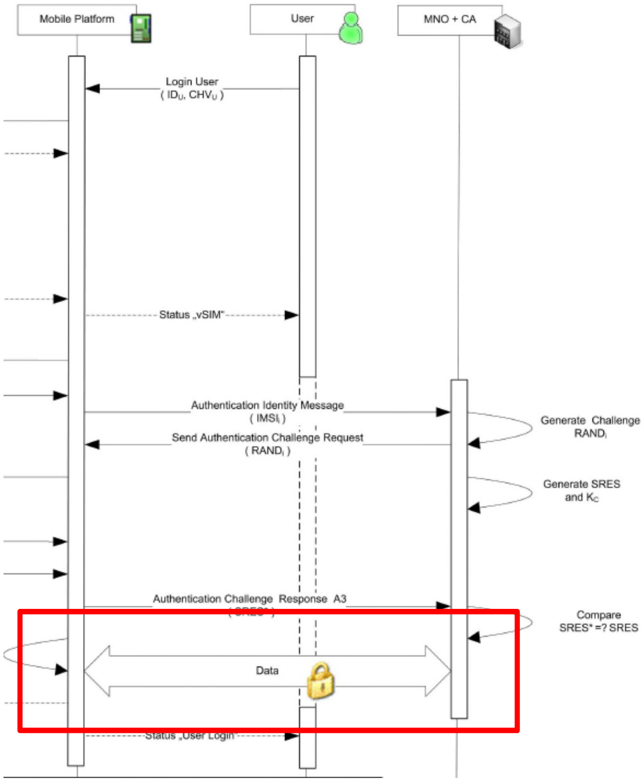
193. To the extent that "relaying the local authentication information request to the remote administration system via the data communication link and obtaining **suitable** local authentication information from the remote administration system via the data communication link" of claim 8 (emphasis added) is limited to the specific embodiment disclosed in the '689 patent at 17:67-18:14, 19:25-47, and 21:5-29, claim 8 is invalid for lack of enablement as discussed in Section X below.

g. "establishing local wireless services provided by the local cellular communication network to the wireless communication client or the extension unit by sending the local authentication information obtained from the remote administration system to the local cellular communication network over signal link;"

194. *Kasper* discloses this element of claim 8. *Kasper* discloses establishing a local wireless service based on the obtained local authentication information. In *Kasper*, the mobile device relays the SRES* message as authentication information to the mobile network operator. After comparing it with the correct SRES, the mobile network operator confirms that "the subscriber is authenticated" and "enables subscriber access to mobile cellular networks" (i.e., local wireless services). *Kasper* at page 59, paras. 6-7, page 39, ¶ 2 ("we present a authentication model that is straight-forward to actual GSM standard and enables subscriber access to mobile cellular networks . . ."), and Figure 3.9.

h. "and providing a communication service to the wireless communication client or the extension unit according to the established local wireless services."

195. *Kasper* discloses this element of claim 8. Based on "access to mobile cellular networks" (i.e., local wireless services), the mobile device in Kasper is provided with communication service. For example, the data service provided to mobile device by mobile network operator as illustrated in Figure 3.9 (partially reproduced below, markups added).



196. Thus, *Kasper* in view of *Walton* teaches all elements of claim 8, and thus renders claim 8 obvious.

2. Claim 11

a. "The wireless communication client or extension unit of claim 8, the memory comprising instructions executable by at least one of the one or more processors for"

197. Claim 11 depends from claim 8 and incorporates all limitations of claim 8, all of which are disclosed, suggested, or taught by *Kasper* in view of *Walton* as explained above in Section IX.E.1.

b. "relaying verification information to the remote administration system, wherein the verification information identifies the wireless communication client or extension unit as being associated with a user account of the remote administration system"

198. *Kasper* discloses this element of claim 11. For example, *Kasper* discloses relaying verification information to the mobile trusted platform. According to *Kasper*, during "Initialization of vSIM Credentials," the user sends "a unique id IDU with a proper password CHVU to the vSIMMGMT service" (i.e., "relaying verification information to the remote administration system" of claim 11). *Kasper* at page 58, ¶ 1.

199. The vSIMMGMT then requests for vSIM credential initialization to the vSIMCORE service and the vSIMCORE service verifies the signature keys held by the vSIMMGMT in order to authenticate the user identity. *Id.* at page 58, ¶ 2. If it is verified, the vSIMCORE unseals the vSIM credential. *Id.* at page 59, ¶ 1. According to Kasper, "[a] vSIM credential CredvSIM is an identity-based identifier that can be used to authenticate a subscriber." *Id.* at page 67, ¶ 3. Therefore, *Kasper* discloses identifying the user being associated with a user account (e.g., vSIM credential initialization).

200. A PHOSITA would be motivated to combine *Kasper* with *Walton* for the same reasons as that set forth in Section IX.E.1. Thus, *Kasper* in view of *Walton* teaches all elements of claim 11, and thus renders claim 11 obvious.

3. Claim 12

201. Claim 12 depends from claim 8 and incorporates all limitations of claim 8, all of

which are disclosed, suggested, or taught by *Kasper* in view of *Walton* as explained above in Section IX.E.1.

202. *Walton* further teaches the additional limitation **"the wireless communication client or the extension unit comprises a foreign wireless communication device not subscribed to the local network**" recited in claim 12. *Walton* provides GSM phone and GSM Roaming Device moving to a "changed network and/or country" (i.e., "not subscribed to the local network" of claim 12). *Walton* at 8:28-9:6 ("…upon detection of a change (which means the phone is roaming), an IP-message with the changed network and/or country is sent . . ."). *Walton* also gives an example of a "GSM phone roam[ing] from The Netherlands to Germany" (i.e., "not subscribed to the local network" of claim 12). *Id*. at 12:31-13:11.

203. A PHOSITA would be motivated to combine *Kasper* with *Walton* for the same reasons as that set forth in Section IX.E.1. Thus, *Kasper* in view of *Walton* teaches all elements of claim 12, and thus renders claim 12 obvious.

4. Claim 13

204. Claim 13 depends from claim 8 and incorporates all limitations of claim 8, all of which are disclosed, suggested, or taught by *Kasper* in view of *Walton* as explained above in Section IX.E.1.

205. *Kasper* further discloses the additional limitation "**requesting access to a desired local wireless service by sending a request to the local cellular communication network over a signal link**" recited in claim 13. For example, *Kasper* discloses "the mobile device requests for authentication at the GSM network" (i.e., "requesting access to a desired local wireless service" of claim 13). *Kasper* at page 59, ¶ 4. More specifically, the mobile device relays the IMSI as a request from vSIMCORE to the network operator (i.e., sending a request to the local cellular communication network). *Id.* at page 59, ¶ 4.

206. To the extent that the claim limitation “a desired local wireless service” of claim 13 is limited to a local wireless service selected based on costs, *Walton* discloses the selection of preferred service according to costs, where it is preferred to “reroute mobile phone voice and data communication based on the lowest cost mobile operator for local calls and data whether the user is within the home network/country or in a foreign network/country.” *Walton* at 3:21-24. Therefore, the “lowest cost mobile operator for local calls and data” corresponds to “a desired local wireless service” of claim 13.

207. A PHOSITA would be motivated to combine *Kasper* with *Walton* for the same reasons as that set forth in Section IX.E.1. Thus, *Kasper* in view of *Walton* teaches all elements of claim 13, and thus renders claim 13 obvious.

X. CLAIM 8 IS INVALID UNDER 35 U.S.C. 112

208. Claim 8 is further invalid because it lacks enablement under 35 U.S.C. § 112, first paragraph, in the ’689 patent specification, to the extent that “relaying the local authentication information request to the remote administration system via the data communication link and obtaining **suitable** local authentication information from the remote administration system via the data communication link” of claim 8 is limited to the specific embodiment disclosed in the ’689 patent at 17:67-18:14, 19:25-47, and 21:5-29.

209. The specification of the ’689 patent provides the following description of “obtaining **suitable** local authentication information from the remote administration system” of claim 8:

> If the subscriber (or wireless communication client) is verified, the authentication server 118 of the administration system 116 obtains